WE CLAIM:

1. An integrated circuit for selectively encrypting plaintext data received from a first device to produce encrypted data to send to a second device, the integrated circuit comprising:

controllable encryption circuitry comprising:

a data input;

an enable input;

a data output;

a plaintext input for providing the plaintext data to the data input;

an encrypted text output for providing the encrypted data from the data output;

a first control input for receiving a first device authentication signal for authenticating the first device; and

a first verification circuit, responsive to the first device authentication signal, for producing a first verification signal for use in controlling the enable input of the encryption circuitry to enable the encryption circuitry to provide the encrypted data via the encrypted text output.

2. The integrated circuit as recited in claim 1, further comprising:

a second control input for receiving a second device authentication signal authenticating the second device;

a second verification circuit responsive to the second device authentication signal for producing a second verification signal; and

a gating circuit responsive to the first and second verification signals for applying an enable signal to the enable input to cause the controllable encryption circuitry to provide the encrypted data via the encrypted text output.

3. The integrated circuit as recited in claim 1, wherein:

the first device authentication signal comprises a device identifier; and

the first verification circuit verifies the first device by comparing the device identifier to a corresponding expected device identifier.

4. The integrated circuit as recited in claim 3, wherein the expected device identifier is hardwired into the integrated circuit.

5. The integrated circuit as recited in claim 3, wherein:

the second device is a non-volatile memory; and

the expected device identifier is stored on the non-volatile memory.

6. The integrated circuit as recited in claim 1, wherein:

the first device authentication signal comprises a message authentication code generated over the plaintext data using a device key; and

the first verification circuit verifies the first device by verifying the message authentication code using an internal key.

7. The integrated circuit as recited in claim 1, wherein:

the first device is a signal processing circuit; and

the second device is a non-volatile memory.

8. A method of controlling encryption circuitry within an integrated circuit by selectively encrypting plaintext data received from a first device to produce encrypted data to send to a second device, the method comprising the steps of:

receiving the plaintext data from the first device;

receiving a first device authentication signal for authenticating the first device;

producing a first verification signal in response to the first device authentication signal; and

enabling the encryption circuitry in response to the first verification signal to provide the encrypted data to the second device.

9. The method of controlling encryption circuitry as recited in claim 8, further comprising the steps of:

receiving a second device authentication signal authenticating the second device;

producing a second verification signal in response to the second device authentication signal; and

enabling the encryption circuitry in response to the first and second verification signals to provide the encrypted data to the second device.

10. The method of controlling encryption circuitry as recited in claim 8, wherein:

the first device authentication signal comprises a device identifier; and

the step of producing a first verification signal in response to the first device authentication signal comprises the step of comparing the device identifier to a corresponding expected device identifier.

11. The method of controlling encryption circuitry as recited in claim 10, wherein the expected device identifier is hardwired into an integrated circuit.

12. The method of controlling encryption circuitry as recited in claim 10, wherein:

the second device is a non-volatile memory; and

the expected device identifier is stored on the non-volatile memory.

13. The method of controlling encryption circuitry as recited in claim 8, wherein: the first device authentication signal comprises a message authentication code generated over the plaintext data using a device key; and the step of producing a first verification signal in response to the first device authentication signal comprises the step of verifying the message authentication code using an internal key.

14. The method of controlling encryption circuitry as recited in claim 8, wherein: the first device is a signal processing circuit; and the second device is a non-volatile memory.